Accès SSH

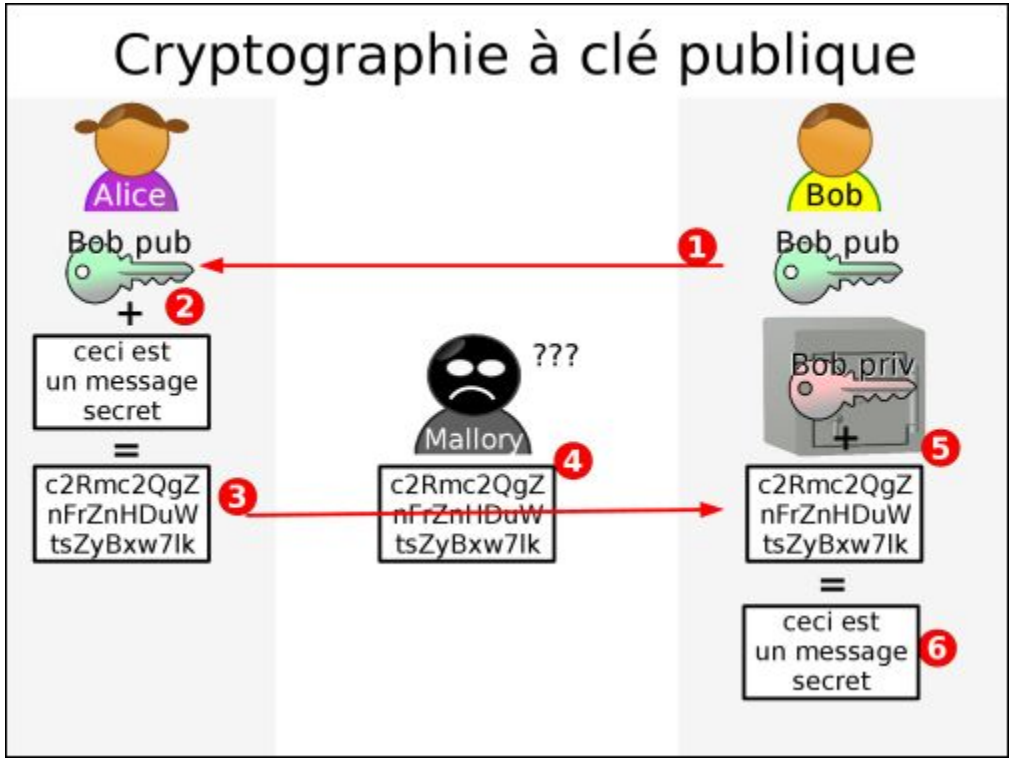
Où l'on accèdera à son système à distance

Qu'est ce que SSH ?

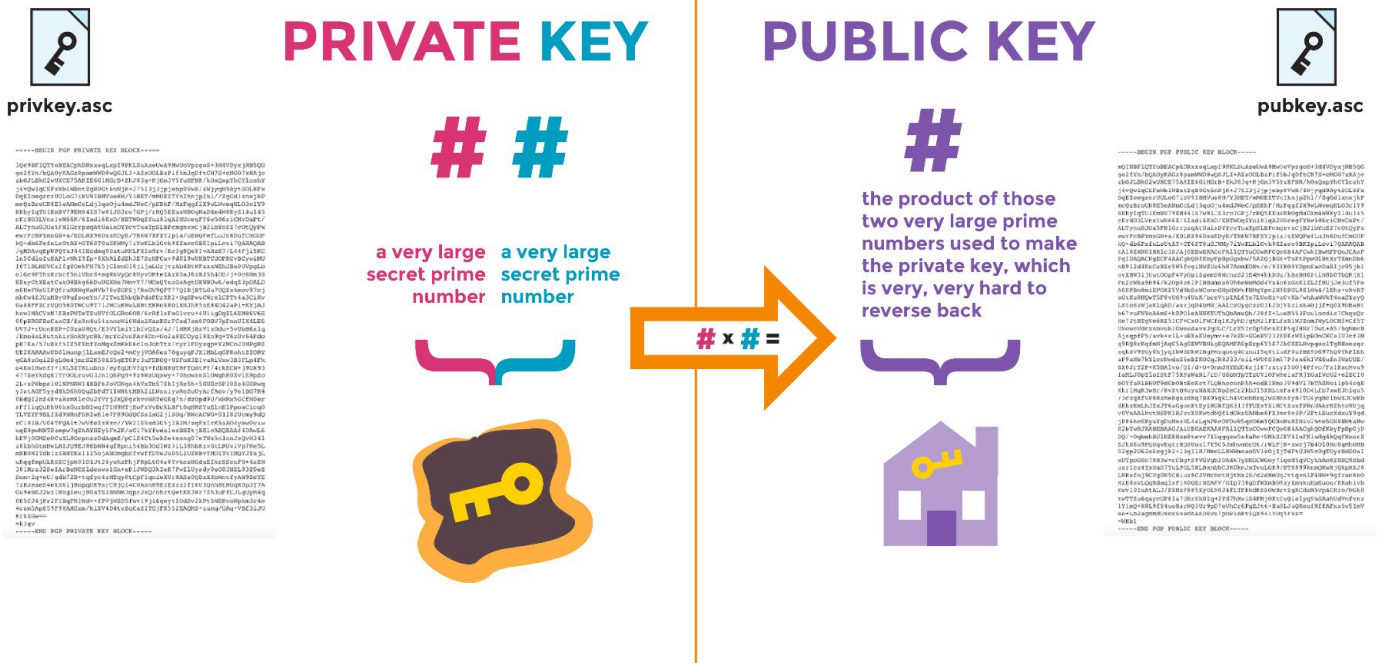
Secure Shell (SSH) est à la fois un programme informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite, tous les segments TCP sont authentifiés et chiffrés. Il devient donc impossible d'utiliser un sniffer pour voir ce que fait l'utilisateur.

Le protocole SSH a été conçu avec l'objectif de remplacer les différents protocoles non chiffrés comme rlogin, telnet, rcp et rsh.

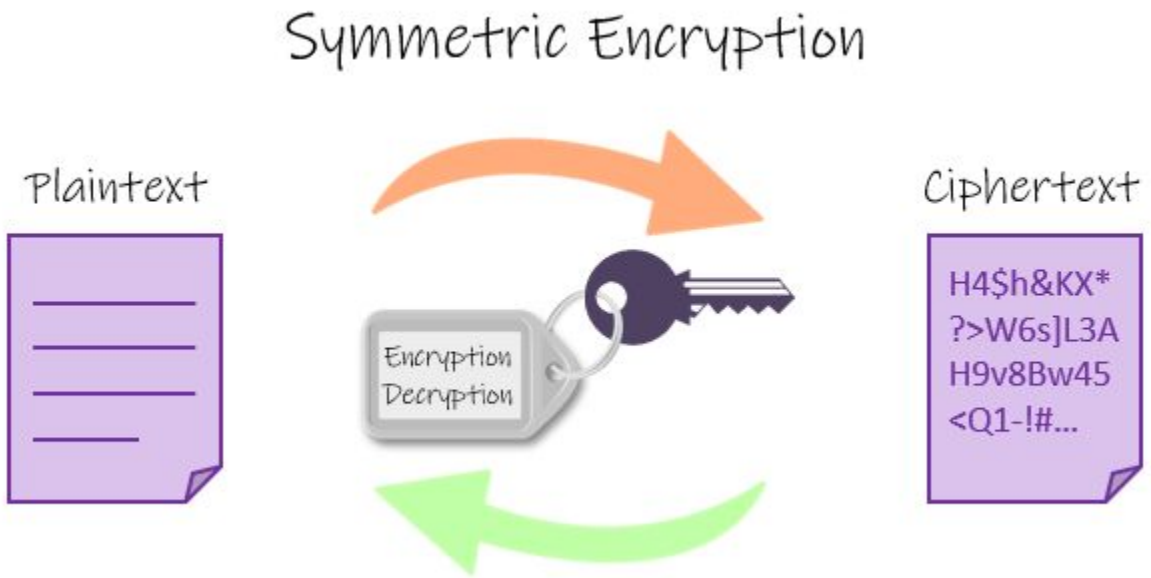
Comment marche la cryptographie à clef publique ?



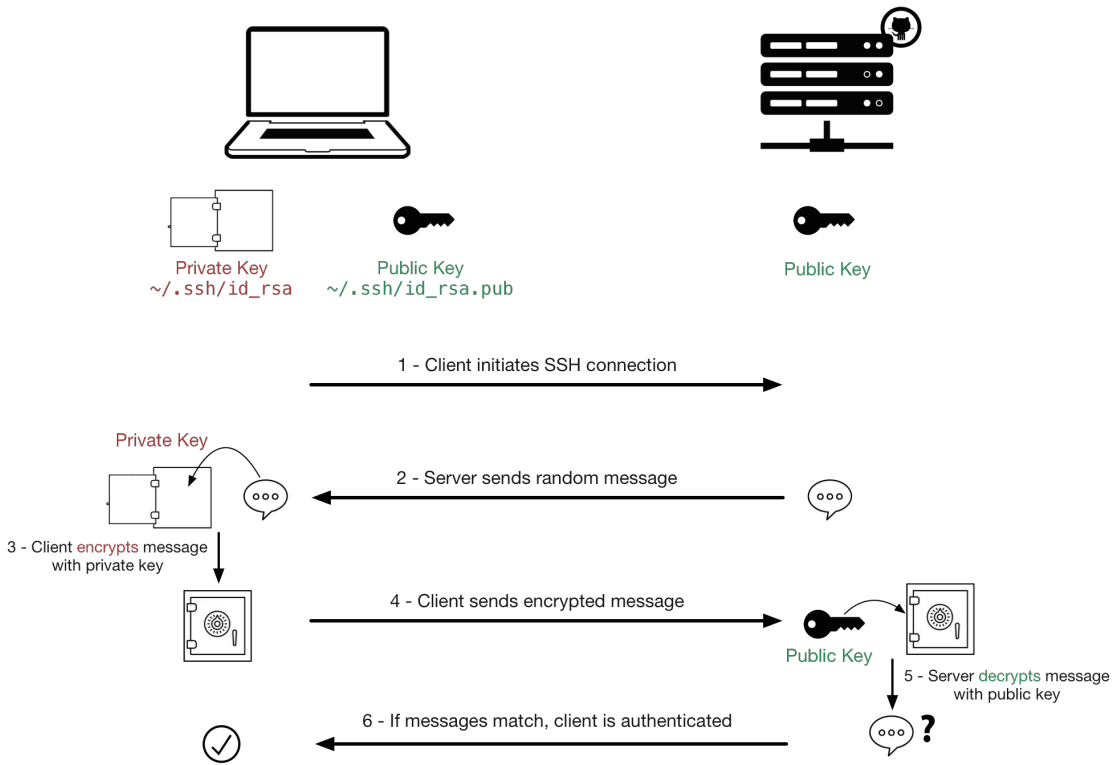
Pourquoi ça marche dans un sens et pas dans l'autre ?



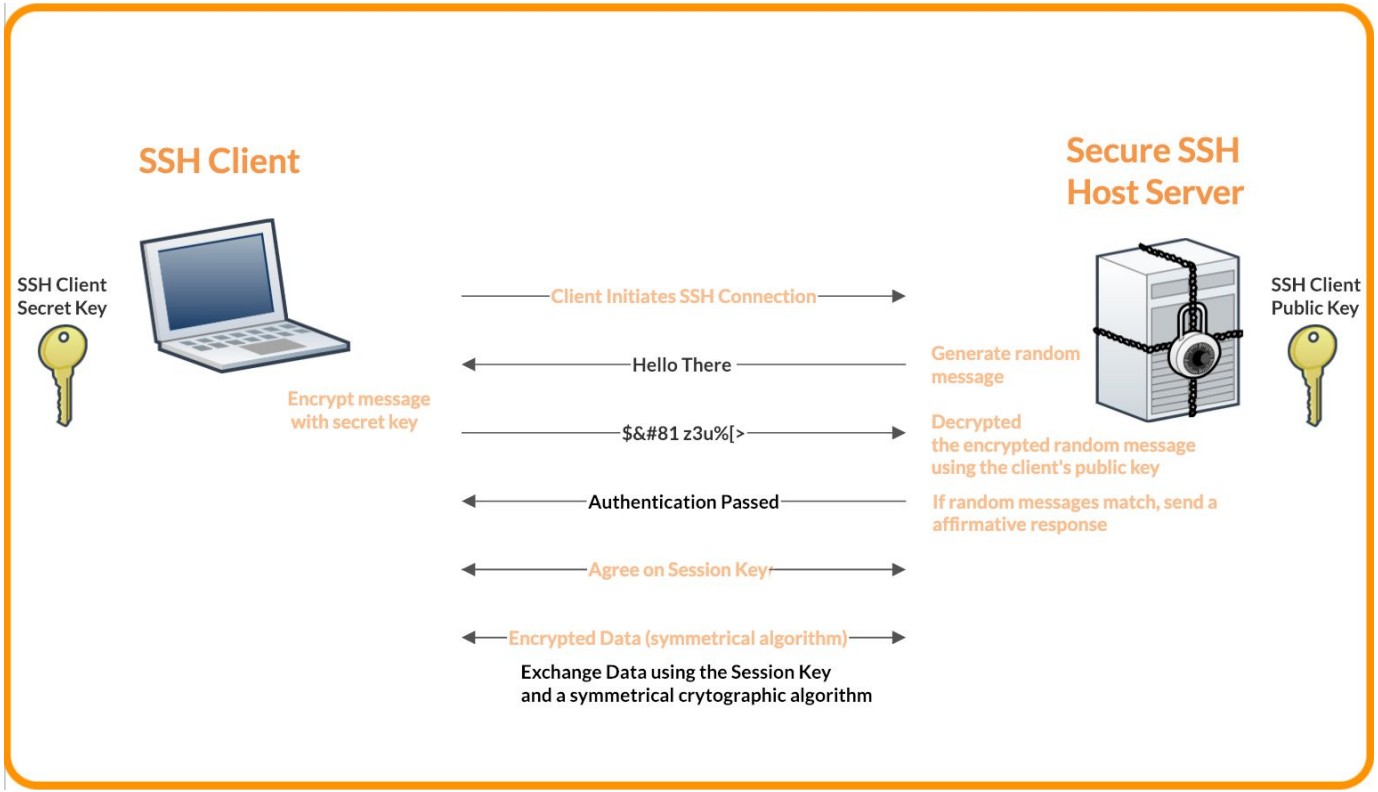
Comprendre l'encryption symétrique



SSH AUTHENTIFICATION



Pour résumer



Utilisation de SSH avec login / password

- Le service SSH est actif par défaut sur votre carte Jetson Nano (mais pas sur votre VM)
- ssh username@ip
- Saisie du mot de passe
- Connexion à la machine

```
❯ ssh afauvel@192.168.64.201
afauvel@192.168.64.201's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/L
```

Inconvénients :

- Il faut saisir son mot de passe à chaque connexion
- Si on a mis un mot de passe peu complexe, la sécurité est faible
- Si le mot de passe est compromis, l'attaquant peut se connecter physiquement et via SSH à la machine

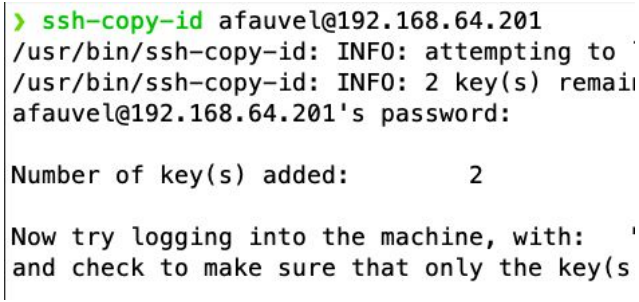
Utilisation de SSH avec des clefs - Générer sa clef

- Générer sa clef SSH (utiliser du chiffrement RSA et protéger la clef avec une passphrase)
- ssh-keygen -t rsa
  - nb : cette commande peut varier selon le système
  - nb2 : Windows intègre désormais nativement la commande SSH
- Nous obtenons deux clefs
  - La clef privée qui ne doit jamais bouger de votre machine
  - La clef publique qui peut être librement partagée

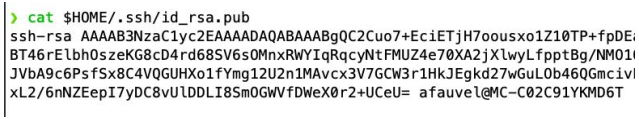
```
afauvel@axel-jetson:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/afauvel/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/afauvel/.ssh/id_rsa.
Your public key has been saved in /home/afauvel/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:voNlaFTINFSIdeGd+qyROVr5MOuQAbPP0vPDtYcQrKg afauvel@axel-jetson
The key's randomart image is:
+---[RSA 2048]----+
|     *=++.       |
|    . ++.. .     |
|    o  o. o      |
|     +. o.       |
|    .o.oS.       |
|    .++++*.      |
|   ...B=@ooo     |
|  E  ..*+Xo .    |
|      ..*o..     |
+----[SHA256]-----+
```

Utilisation de SSH avec des clefs - Copier sa clef

- Option n°1 : je connais le mot de passe de l'utilisateur avec lequel je souhaite me connecter
  - ssh-copy-id username@ip



- Option n°2 : je fournis ma clef à la personne responsable de déployer les clefs sur les machines
  - cat $HOME/.ssh/id_rsa.pub
  - J'envoie ça à la personne qui va la copier sur la machine



Utilisation de SSH avec des clefs - Se connecter

- `ssh username@ip`

PAF chocapics

Exercice

- installez le paquet ssh
- connectez vous à votre VM depuis votre système en utilisant login/password (rappelez vous, lors de l'installation de la VM, nous avions fait une redirection de ports)
- Déconnectez vous de votre VM
- Générez une paire de clefs sur votre système
- Autorisez votre clef publique sur votre VM
- Connectez vous à votre VM en utilisant votre clef privée

Pour aller plus loin

Comment marche SSH : https://www.hostinger.com/tutorials/ssh-tutorial-how-does-ssh-work

Config SSH : https://linuxize.com/post/using-the-ssh-config-file/

Agent SSH : https://www.ssh.com/academy/ssh/agent